Делимость

Определение

Пусть $a, b \in \mathbb{Z}$, $b \neq 0$. Тогда a *делится* на b (обозначение: $a \,\vdots\, b$) или, что то же самое, b *делит* a (обозначение: $b \mid a$), если $a = bc$, где $c \in \mathbb{Z}$.
Если $a \,\vdots\, b$, то b — *делитель* a.

Свойство 1

Если $a \,\vdots\, b$ и $b \,\vdots\, c$, то $a \,\vdots\, c$.

Доказательство. Тогда $a = kb$ и $b = nc$, где $k, n \in \mathbb{Z}$, откуда следует $a = knc$. □

Свойство 2

Пусть $a, b \,\vdots\, d$, а $x, y \in \mathbb{Z}$. Тогда $ax + by \,\vdots\, d$.

Доказательство. Тогда $a = kd$ и $b = nd$, где $k, n \in \mathbb{Z}$, откуда следует $ax + by = (kx + ny)d$. □

Свойство 3

Пусть $a, d \in \mathbb{N}$, $a \,\vdots\, d$. Тогда $a \geq d$.

Доказательство. Тогда $a = kd$, где $k \in \mathbb{N}$, откуда следует $a = kd \geq d$. □

Теорема о делении с остатком

Теорема 1

Пусть $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Тогда существуют единственные такие $q, r \in \mathbb{Z}$, что $0 \leq r < b$ и $a = bq + r$.

• Число r называется *остатком* от деления a на b.

Доказательство. $\exists$. Пусть q — такое целое число, что $bq \leq a < b(q+1)$, а $r = a - bq$. Тогда $0 \leq r < b$ (вычтем из всех трех частей первого неравенства bq).

! • Пусть $a = bq_1 + r_1 = bq_2 + r_2$, причем $0 \leq r_1 < b$ и $0 \leq r_2 < b$.

• НУО $r_1 > r_2$. Тогда $0 < r_1 - r_2 < b$.

• С другой стороны, $r_1 - r_2 = b(q_2 - q_1) \geq b$. Противоречие. □

bq ≤ a < b(q+1)| –bq
0 ≤ r < bq+b – bq => 0 ≤ r < b

r1 > r2 => 0 < r1 – r2 < b
(т.к. r1 != r2 => один из них будет больше)
r1 – r2 = a – bq1 – a + bq2 = b(q2 – q1) ≥ b
(т.к. q2 != q1 – количество раз, сколько b входит в a)

НОД

Определение

Пусть $a_1, \dots, a_n \in \mathbb{Z}$. Обозначим через $\mathrm{OD}(a_1, \dots, a_n)$ множество всех общих делителей этих чисел, а через $(a_1, \dots, a_n)$ — их НОД (наибольший из общих делителей).

Свойство 1

Если $b \in \mathbb{N}$. $a \,\vdots\, b$, то $\mathrm{OD}(a, b)$ — это все делители b и $(a, b) = b$.

Пример: b = 4, a = 16, очевидно, что OD (1,2, 4)

Доказательство. • Если d — общий делитель a и b, то d — делитель b.

• Если d — делитель b, то $a \,\vdots\, d$ по свойству 1 делимости. Значит, d — общий делитель a и b.

Также рассмотрим на примере:
1, 2, 4 – общие делители 4 и 16, то 1, 2, 4 – делители 4

1, 2, 4 – делители 4, => 1,2,4 – делители a, => это общие делители

Свойство 2

Пусть $a, b, c, k \in \mathbb{Z}$, $c = a + kb$. Тогда $\mathrm{OD}(a, b) = \mathrm{OD}(c, b)$, а следовательно, и $(a, b) = (c, b)$.

Пример: a = 2, b = 3, k = 4
c = 2 + 4*3 = 14
OD(a,b) = 1 = OD (14, 3) = 1

Пример 2: a = 2, b = 6, k = 4
c = 2 + 4*6 = 26
OD(a,b) = 1, 2 = OD (26, 6) = 1,2

Доказательство. • Пусть $d \in \mathrm{OD}(a, b)$. Тогда $c \,\vdots\, d$, а значит, $d \in \mathrm{OD}(c, b)$.

• Наоборот, если $d \in \mathrm{OD}(c, b)$, то $a = c - kb \,\vdots\, d$, а значит, $d \in \mathrm{OD}(a, b)$.

Если d ∈ OD (a,b) => c = a + kb ⋮ d => d ∈ OD (c,b)

Если d ∈ OD (c,b) => a = c - kb ⋮ d => d ∈ OD (a,b)